数理解析研究所講究録
310巻 1977年 105-115

有限体の楕円関数の計算
(実験整数論の一例題)

慶大 工学部　　高橋 秀俊

整数論の問題，たとえば素数の分布，代数体の構造などに対して，計算機を使ってたくさんの具体例をつくり，一般的な法則をみつけるための手掛りとすることは，実験整数論などと呼ばれて，いろいろと例がある．ここではその一つとして，有限体における楕円関数についてその実例をつくってしらべたことについて報告する．

楕円関数は通常は楕円積分の逆関数として，または2重周期関数を生成する極表示，因数表示等によって定義されるが，また加法定理から定義することも可能である．加法定理は純代数的な関係であるので，これによれば離散系であるところの有限体を値域とする楕円関数を導入することができる．

加法定理の形

いま，加法定理を

(1) $$f(u+v)=F(f(u),\ f(v))$$

とする．ここで v の方は一つのパラメーターと考えて，

$$f(u)=x, \quad f(u+v)=z$$

と書いて，（1）を x と z の間の関係としてとらえると，z は

$$(2) \qquad z=F_v(x)=\frac{Q(x)\pm\sqrt{D(x)}}{P(x)}$$

のような形に書ける．即ち，位数2の楕円関数の加法定理は2次の無理式（平方根号が1個入った式）であらわされる．ここで $D(x)$ は解析学で楕円関数を $u=\int dx/\sqrt{D(x)}$ の逆関数として定義するときの3次または4次の多項式 $D(x)$ である．

（2）は x の2価関数であるが，その二つの価はそれぞれ $f(u+v)$，$f(u-v)$ のいずれかをあらわすことが示される．また，（2）を方程式の形になおすと

$$(3) \qquad \Phi_v(x,z)=x^2z^2+axz(x+z)+b(x^2+z^2)$$
$$+cxz+d(x+z)+e=0$$

のように書ける．即ち，$F_v(x)$ およびその逆関数がいずれも2価であることから，$\Phi_v(x,z)$ は z，x のおのおのに対して2次（双2次）の多項式であり，しかも x，z に対して対称な式となる．逆に，（3）の形の式はいつも一つの楕円関数の加法定理をあらわすことも知られている．

E 数列の生成

以上のことから，有限体 $GF(p^m)$ を値域とする離散的な

楕円関数を生成する次のようなアルゴリズムが出てくる。

"判別式" $D(x)$ を定めておく．これから定義される楕円関数 $f(u)$ が $\wp$ 関数，cn関数などのように u の偶関数となるように u の原点を選ぶものとする．そのとき加法定理の $\Phi_v(x,z)$ の係数は $y=f(v)$ の有理式となり，したがって $y\in GF(p^m)$ を与えれば $GF(p^m)$ 中の係数をもつ加法定理が得られる．こうして得た式を

$$z=F(x,y)$$

とする．そこでまず，$x=f(u)$ を適宜に与えて，それから

$$F(x,y)=\begin{cases} f(u+v)=x_1 \\ f(u-v)=x_{-1} \end{cases}$$

を得る．次に x_1 から

$$F(x_1,y)=\begin{cases} f(u+v+v)=f(u+2v)=x_2 \\ f(u+v-v)=f(u)=x \end{cases}$$

を得る．x は既知で，x_2 が新らしい値であるが，2次方程式の1根が既知なのだから，x_2 は x_1 と x から有理的に求まる．以下同様にして $f(u+kv)=x_k$ を求めて行く．こうして得た数列 $x,x_1,x_2,\cdots$ は元の種類が有限だからどこかで循環する．このような循環数列を<u>E 数列</u>と呼ぼう．

ここで E 数列の元が"実在する"（つまり $GF(p^m)$ 中に存在する）ためには x_k から x_{k+1} を求める式で $D(x_k)$ が平方

剰余になっていなければならない．そしてそのとき，一つのx_kからx_{k+1}として二通りの値がきまる．そのどちらを取るかを決めるのはx_{k-1}であるが，これをもx_kの性質と考え，つまり，複素解析のリーマン面上の点のように，x_kの数値と共に$\sqrt{D(x_k)}$の符号のどちらを取るかの情報をも含ませた実体概念を考えて，これを“点”と呼ぶことにする．すると，$D(x)=$平方剰余であるような$x \in GF(p^m)$の一つ一つにはそれぞれ2個の点が対応する．そのほか$D(x)=0$となるxの値（$D(x)$が3次式のときは$x=\infty$も含む）にはそれぞれ1点が対応する．そのような“点”の集合をE_D^+と書く．またその元の数をN_D^+とする．

さて，上のようにして得たE数列がE_D^+のすべての元を尽していればよし，そうでないときは，残りの元の一つをxとして，新らしいE数列がつくられる．こうして何本かのE数列をつくることにより，E_D^+の元は全部使われる．これらのE数列の長さ（周期）ℓはすべて等しく，したがって

(4) $\qquad N_D^+ = n\ell \qquad$ （nは数列の数）

である．

次に，同じ$D(x)$でyの値を変えて得られる新らしい加法関係を用いて，同様にして新らしいE数列が得られる．それは既に得たE数列の元を等間隔にとびこしてたどったに過

ぎない場合もあるが，また前には別のE数列に属していた元を横につらねるようなものも得られる．こうして，いろいろのyに対するE数列は，E_D^+ の元の全体を一つの格子(加群)の上に配置することになる．即ち，一つの加群を変域とし，E_D^+を値域とする関数として，有限体の楕円関数が定義される．

<u>例1</u>　基礎体：$GF(13)$．　平方剰余$=\{1,3,4,9,10,12\}$

$$D(x)=x^3+x+1=(x-7)(x^2+7x+11)$$

$$D(x)\text{の値} = \underline{1},\ \underline{3},\ 11,\ 5,\ \underline{4},\ \underline{1},\ 2,\ \underline{0},\ \underline{1},\ 11,\ \underline{10},\ \underline{4},\ \underline{12}$$

$$E_D^+=\{0,1,4,5,8,10,11,12\}\times 2\cup\{7,\infty\}\qquad N_D^+=18$$

$$F(x,y)=\left(\frac{\sqrt{D(x)}-\sqrt{D(y)}}{x-y}\right)^2-x-y\quad(\wp\text{関数の加法定理})$$

$y=1$ を選ぶと　$F(x,1)=\left(\dfrac{\sqrt{x^3+x+1}-4}{x-1}\right)^2-x-1$

これから　E数列 $\cdots-\infty-1-8-0-11-5-10-12-$

$-4-7-4-12-10-5-11-0-8-1-\infty-\cdots$

が得られる．周期$=18$ で，E_D^+ の元全体を尽しているから，この場合の加群は巡回群である．数列は∞，7のところを中心に対称．

<u>もう一つのE数列</u>

$GF(p^m)$の中でE_D^+に洩れた点，つまり$D(x)=$平方非剰余　であるような点の集合をE_D^-と書くと，その元の数

は $N_D^- = 2(p^m+1) - N_D^+$ である．ここで p^m+1 というのは射影的に見た $GF(p^m)$ の元の数（∞ が含まれる）であって，その各元が2回ずつあらわれるので $N_D^+ + N_D^- = 2(p^m+1)$ となるのである．さて，c を $GF(p^m)$ での平方非剰余数の一つとしたとき，

$$z = \frac{Q(x) + \sqrt{cD(x)}}{P(x)}$$

の形の加法関係を使えば $\mathbf{E}_D^-$ の数から成る E 数列をつくることができる．こうして得た楕円関数の諸性質は $\mathbf{E}_D^+$ の場合と全く変らない．

例 1.　$GF(13)$.　$cD(x) = 2(x^3+x+1)$

◎　$\mathbf{E}_D^- = \{2, 3, 6, 9\} \times 2 \cup \{7, \infty\}$　$N_D^- = 10$

$y=3$ を選ぶと　$F(x,3) = \frac{1}{2}\left(\frac{\sqrt{2(x^3+x+1)} - 6}{x-3}\right)^2 - x - 3$

E 数列：　$\infty - 3 - 2 - 6 - 9 - 7 - 9 - 6 - 2 - 3 - \infty$

これと前節の $\mathbf{E}_D^+$ の E 数列とを合わせると，$GF(13)$ の数（および ∞）が全部2回ずつあらわれる．

例 2.　$GF(13)$.　$D(x) = x^3 + 2$

◎　$\mathbf{E}_D^+ = \{1, 2, 3, 4, 5, 6, 9, 10, 12\} \times 2 \cup \{\infty\}$　$N_D^+ = 19$

$y=1$ とすると，　E 数列：$-\infty - 1 - 2 - 6 - 10 - 5 - 4 - 9 - 3 - 12 - 12 - 3 - 9 - \cdots\cdots$

x^3+2 は既約であるから $f(u)$ の極値，つまり折返点は ∞ 以外にない．そこで周期が奇数となる．次に

◎ $E_D^- = \{0, 7, 8, 11\}\times 2 \cup \{\infty\}$　　　$N_D^- = 9$

$y=0$ とすると，$-\infty-0-0-\infty-$，$-7-8-11-7-$

2番目の数列は非対称であるから，逆読みしたものも存在する．また，$y=7$ とすると，$-\infty-7-7-\infty-$

以上から，次のような，2次元加群の上の関数が得られる．

$$
\begin{array}{ccccccccc}
 & | & & | & & | & & | & \\
- & \infty & - & 0 & - & 0 & - & \infty & - \\
 & | & & | & & | & & | & \\
- & 7 & - & 8 & - & 11 & - & 7 & - \\
 & | & & | & & | & & | & \\
- & 7 & - & 11 & - & 8 & - & 7 & - \\
 & | & & | & & | & & | & \\
- & \infty & - & 0 & - & 0 & - & \infty & - \\
 & | & & | & & | & & | &
\end{array}
$$
」

$D(x)$ が1次因子に分解されるときは，$l\times 2$ の形の2次元加群になる．しかし上のような $l\times l'$ のどちらも >2 であるような2次元加群があらわれる例は比較的少ない．

3次元以上の加群は決してあらわれない．これは複素関数としての楕円関数が2重周期であることと対応する．しかし，上例のように，“実”の値をとる点が2次元配列をとるのは，複素関数の場合には見られぬ状況である．

楕円関数の分類

基礎体をきめ，$D(x)$ を与えると，一つの楕円関数が定まる．$D(x)$ は定数因子を除いて4個のパラメーターがあるか

ら，$GF(p)$ において約 p^4 種類の楕円関数が得られるわけである．しかし，それらの中には x に対する一次変換で互に移り変るものが含まれているから，それら互に同型のものを一つに数えると，異る楕円関数の数は p の程度となる．それらはいわゆる絶対不変量 J によって区別されることも，複素関数の場合と同じである．実際は一次変換を"実"の変換に制限する方が都合がよく，そうすると異る関数の数は約 $2p$ になる．（正確には，$p\equiv 1 \bmod 3$ のとき $2p+3$ 個，$p\equiv -1 \bmod 3$ のとき $2p+1$ 個）そして，それぞれに E_D^+ に属するものと E_D^- に属するものの両方がある．

$D(x)$ の性質，主として $D(x)$ の既約因子の次数のパターンによって，楕円関数の型が分けられる．因子の次数をならべてたとえば〈112〉というような書き方をすると，

〈1111〉，〈112〉，〈22〉，〈13〉，〈4〉

の5種の型がある．ここで3次の $D(x)$ は ∞ を零点とする因子が別にあると解釈する．ここで，〈22〉型，〈4〉型は実の変換で Weierstrass 標準形にすることができないが，虚の変換によって，それぞれ〈1111〉型，〈112〉型の標準形に変換され，その際，周期性は保存される．

主な特徴を挙げると，1．〈1111〉型（および〈22〉型）では加群は常に2次元的である．但し多くの場合，一方の周

期は2である．2．<13>型では周期は常に奇数である．等である．

計算機による計算

GF(p) を基礎体とする楕円関数の性質を，p は 7 から 43 までのすべての素数について，そしてすべての J について，具体的な計算によってしらべた．その他 p=61, 97, 113 等についても一部のものを計算した．その際の興味の中心は，短かい方の周期が2よりも長いような2次元加群があらわれる場合にあった．そのような加群の出現頻度は比較的少く，そして $J=0$ $(D(x)=x^3+a)$, $J=1$ $(D(x)=x^3+ax)$ の場合に比較的現われ易い傾向が見られる．下に若干の例を示す．

p	$D(x)$ とその分解	$N_D^+=n\times l$
7	$x^3+2=$ 既約	$9=3\times3$
13	$x^3+8=(x+2)(x+5)(x+6)$	$16=4\times4$
	$x^3+3=$ 既約	$9=3\times3$
	$x^3+2x=x(x^2+2)$	$18=3\times6$
17	$x^3+x=x(x+4)(x-4)$	$16=4\times4$
19	$x^3+2=$ 既約	$27=3\times9$
	$x^3-x+1=(x+6)(x^2-6x+3)$	$18=3\times6$

29	$x^3+4x+22=(x+4)(x+8)(x-12)$	$32=4\times 8$
31	$x^3+1=(x+1)(x+5)(x-6)$ $x^3+26=$ 既約 $x^3+x+11=(x-16)(x^2+16x+9)$ $x^3-x+10=$ 既約	$36=6\times 6$ $25=5\times 5$ $36=3\times 12$ $27=3\times 9$
37	$x^3+1=(x+1)(x+10)(x-11)$ $x^3+16=$ 既約 $x^3+x=x(x+6)(x-6)$ $x^3+4x+1=(x+7)(x^2-7x-15)$ $x^3+8x+30=(x-10)(x-13)(x-14)$ $x^3+2x+14=$ 既約	$48=4\times 12$ $27=3\times 9$ $36=6\times 6$ $36=3\times 12$ $32=4\times 8$ $45=3\times 15$
41	$x^3+x=x(x+9)(x-9)$ $x^3+27x=x(x^2+27)$ $x^3+3x+3=(x+8)(x+16)(x+17)$	$32=4\times 8$ $50=5\times 10$ $48=4\times 12$
43	$x^3+1=(x+1)(x+6)(x-7)$ $x^3+3=$ 既約 $x^3+x+15=(x-17)(x^2+17x+32)$ $x^3-x+8=(x-7)(x^2+7x+5)$ $x^3-x+14=$既約	$36=6\times 6$ $49=7\times 7$ $54=3\times 18$ $36=3\times 12$ $45=3\times 15$

以上の結果を見てわかる一つの著しい事実は，加群の短かい方の周期 n が常に $p-1$ の約数であることである．上表では $n=3, 4, 5, 6, 7$ のすべてについて成立している．($n=2$ については自明．) 短周期が n ということは，周期を n 等分する n^2 個の点での関数の値 (n 位の特殊除法方程式の根) がすべて $GF(p)$ の中にあるということであるが，一方，$n|p-1$ は円周等分方程式 $x^n-1=0$ の根がすべて $GF(p)$ の中にあるための必要十分条件である．この二つの非常に似た方程式の根の性質の間にこのような相関関係があることは極めて自然なことであり，恐らく周知の事柄であろうと思われるが，この方面を専攻されている方の御教示が得られれば幸である．